CAN YOU HEAR ME NOW?

ELECTROMAGNETIC SPECTRUM: CRITICAL TO OUR NATION'S SECURITY AND ECONOMY

By the DON CIO Telecom/RF Spectrum/Wireless Team

New innovative technologies to improve wireless efficiency will be needed to ensure America's future security and economic strength ...

Increasingly, our lives, lifestyles, culture and economy depend on wireless devices. Wireless devices enable us to remotely monitor our sleeping children, turn on the television without leaving the couch, make phone calls whenever and wherever, pass through toll booths without stopping, and use our laptops and personal digital assistants virtually anywhere. These devices, and many others in our modern world, work because of the electromagnetic spectrum.

Electromagnetic spectrum — usually referred to as "spectrum" — encompasses radio waves, infrared, visible light, ultraviolet light, x-rays, gamma rays and cosmic rays. Radio waves are an incredibly versatile area of the spectrum and make much of our modern communication possible, including television, AM and FM radio bands and satellite radio broadcasting. While spectrum makes our lives more enjoyable, it is, in fact, critical to our modern quality of life.

Modern health care depends on spectrum to operate medical monitoring systems. Public utilities use spectrum to remotely control pipeline valves that direct the flow of our water, electricity and gas. Transportation systems rely on spectrum for cargo tracking, air traffic control and security sensors.

Firefighters, police and emergency service personnel require spectrum for rapid communication, location positioning and other services. Additionally, spectrum allows manufacturers, shippers and merchants to monitor the location of products using advanced identification technologies, such as radio frequency identification (RFID).

Warfighter Reliance on Spectrum

Our Naval forces are especially reliant on spectrum. Using RFID technology, the Navy and Marine Corps track shipments of critical supplies and confirm patient identity and enter diagnosis and treatment information. In addition to implementing commercial technologies, our Naval forces have unique spectrum requirements. Communications; radar; air and fleet defense; weapons guidance; command and control; and many other systems rely on spectrum to function. In fact, conducting network-centric warfare is impossible without spectrum.

Marine Expeditionary Forces, with integrated aircraft and combat service support, along with Navy SEAL teams, submarines and carrier strike groups are often the first to arrive in theater and must rely on spectrum to remain highly maneuverable, flexible and tactically effective.

An example of complex spectrum demand is found in a typical naval aircraft — voice communications and digital data links require many wireless devices. Weapons systems with associated fire control radar rely on spectrum for guidance to find and destroy their targets. Such demands have both expanded our military's need for, and increased its dependency on, spectrum.

The Challenge

A critical challenge is that spectrum is a finite resource, and it is in great demand. Without careful planning and implementation, spectrum-dependent systems may unintentionally, yet adversely interfere with each other. For example, a test flight at a naval air station was delayed because of interference to an important ground-based test measurement instrument. The source of the interference was a malfunctioning baby monitor in nearby military housing.

Providing balance between spectrum-dependent devices that make our lives more convenient and those that are critical to our national defense is a growing challenge. New technologies to improve wireless efficiency will be needed to maintain a balance between national defense and economic strength.

In the Department of the Navy (DON), we are constantly exploring technologies that allow us to utilize spectrum in innovative ways. Some of these technologies include:

- Frequency agile technologies that can sense a competing device on the same frequency and instantly switch to available spectrum;
- Software defined radios that can set or alter almost any characteristic of a device, including frequency ranges and power and modulation, simply by loading new software;
- Ultra-wide band devices that can "see through walls" to detect combat threats without entering a building.

In addition to implementing new technology, we must all collaborate in the efficient use of current assets to guarantee dependable spectrum access for everyone.

Coordination of Spectrum Use

The complexity of spectrum coordination is enormous, and it is a global challenge because the DON deploys Marine Corps forces and Navy assets worldwide. Careful and constant coordination is required to guarantee that the Department meets it mission.

Through international negotiations, the DON ensures that

Marine Expeditionary Forces, with integrated aircraft and combat service support, along with Navy SEAL teams, submarines and battle groups are often the first to arrive in theater and must rely on spectrum to remain highly maneuverable, flexible and tactically effective.

the spectrum-dependent capabilities of the Navy and Marine Corps are preserved. Because the radio frequency spectrum must be shared among nations, a United Nations agency, the International Telecommunication Union, convenes the World Radiocommunication Conference to modify spectrum allocation as technology and services require.

All members of the United Nations are invited to these conferences and the Department of the Navy Chief Information Officer participates as the Department's national and international representative to these forums.

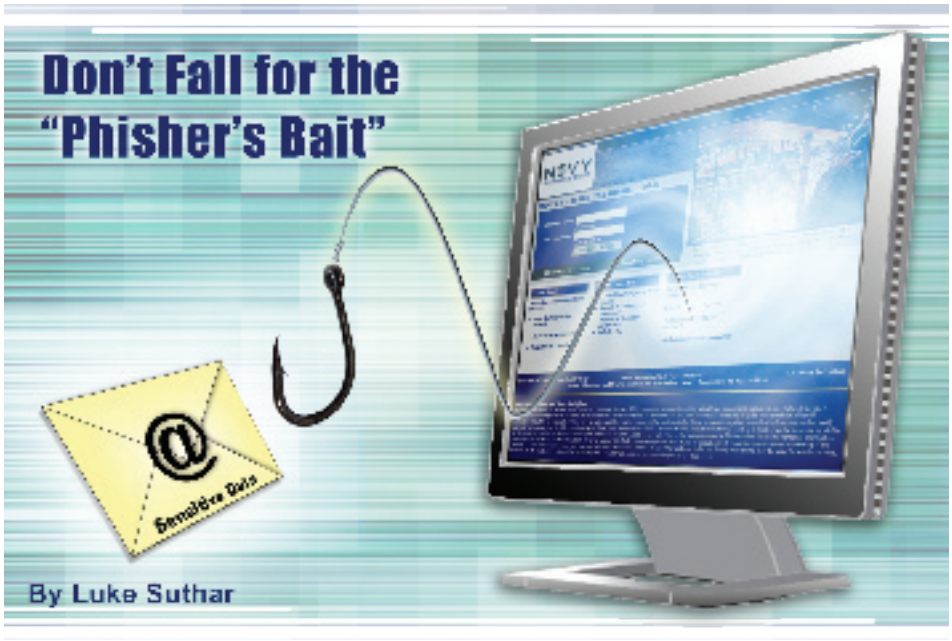
To achieve its goals, the DON strives to improve efficient use of spectrum through collaborative efforts among business, industry, government and other nations.

In order to maintain America's advantage and secure our country's future, we must continue to work to meet our growing national spectrum challenges because electromagnetic spectrum is critical to both our nation's security and economy.

For more information, please contact the DON Spectrum Team at DONSpectrumTeam@navy.mil.

CHIPS

Can You Hear Me Now is a regularly featured column in CHIPS magazine. Please go to the CHIPS Web site at http://www.chips.navy.mil/ and click on the Archives link at the top of the page to view past columns.



Department of the Navy (DON) networks are under continuous attack by an invasion of "spam on steroids." There has been a significant and widespread trend of using bogus e-mails to steal personal information and access critical DON information systems.

The ultimate objective of these Internet intruders is to trick unsuspecting users to open an attachment or click a Web link that will download specialized malicious software onto the computer. This process circumvents existing security measures and allows access to DON data.

The Naval Criminal Investigative Service (NCIS) has observed a growing trend of thousands of malicious e-mails targeting Sailors, Marines, Navy civilian workers and DON contractors, with the potential to compromise a significant number of computers across the Department.

Web Tricks

"Phishing" is a criminal activity in which an adversary attempts to fraudulently acquire sensitive information by impersonating a trustworthy person or organization using, for example, manipulated e-mails that appear to represent the DON, Navy Federal Credit Union, Navy Knowledge Online (NKO) or other familiar institutions.

The ultimate goal of a phishing attempt is to extract information through the contact in order to evade existing security measures and allow access to DON secure information and data. Phishing is typically carried out using two techniques: "spoofing" and "social engineering."

Spoofing an e-mail creates a fraudulent message with an e-mail address and page content that appear to be from a valid source. Often the e-mails contain malicious attachments and links to deceptive Web sites that appear to be an exact duplicate of the authentic Web sites.

Social engineering involves multiple correspondences to potential victims in order to get them to divulge critical and confidential information through trickery. Correspondence includes, but is not limited to, the use of e-mails, telephone calls and personal contact.

Victims are manipulated or tricked into providing personally identifiable information, such as credit card numbers, bank information, Social Security numbers, user IDs and passwords — and possible critical information that could harm the DON network that would not be otherwise easily disclosed.

When spoofing and social engineering are concatenated, the outcome is a new technique, known as "spear phishing" — a mass of manipulative e-mails to unsuspecting recipients who believe the message is authentic and from a trusted sender.

When using spear phishing, offenders adapt to security measures that would otherwise block a majority of these menacing e-mails. This type of attack uses targeted e-mails that are manipulated to